

ON THE COMPLEXITY OF FINITE VALUED FUNCTIONS

SLAVCHO SHTRAKOV AND IVO DAMYANOV

ABSTRACT. The essential variables in a finite function f are defined as variables which occur in f and weigh with the values of that function. The number of essential variables is an important measure of complexity for discrete functions. When replacing some variables in a function with constants the resulting functions are called subfunctions, and when replacing all essential variables in a function with constants we obtain an implementation of this function. Such an implementation corresponds with a path in an ordered decision diagram (ODD) of the function which connects the root with a leaf of the diagram. The sets of essential variables in subfunctions of f are called separable in f . In this paper we study several properties of separable sets of variables in functions which directly impact on the number of implementations and subfunctions in these functions.

We define equivalence relations which classify the functions of k -valued logic into classes with same number of implementations, subfunctions or separable sets. These relations induce three transformation groups which are compared with the lattice of all subgroups of restricted affine group (RAG). This allows us to solve several important computational and combinatorial problems.

1. INTRODUCTION

Understanding the complexity of k -valued functions is still one of the fundamental tasks in the theory of computation. At present, besides classical methods like substitution or degree arguments a bunch of combinatorial and algebraic techniques have been introduced to tackle this extremely difficult problem. There has been significant progress analysing the power of randomness and quantum bits or multiparty communication protocols that help to capture the complexity of switching functions. For tight estimations concerning the basic, most simple model switching circuits there still seems a long way to go (see [4]).

In Section 2 we introduce the basic notation and give definitions of separable sets, subfunctions, etc. The properties of distributive sets of variables with their s -systems are also discussed in Section 2. In Section 3 we study the ordered decomposition trees (ODTs), ordered decision diagrams (ODDs), and implementations of discrete functions. We also discuss several problems with the complexity of representations of functions with respect to their ODDs, subfunctions and separable sets. In Section 4 we classify discrete functions by transformation groups and equivalence relations concerning the number of implementations, subfunctions and separable sets in functions. In Section 5 we use these results to classify all boolean (switching) functions with "small" number of its essential variables. Here we calculate the number of equivalence classes and cardinalities of equivalence classes of boolean functions depending on 3, 4 and 5 variables.

Key words and phrases. Ordered decision diagram; implementation; subfunction; separable set.

2. SEPARABLE AND DISTRIBUTIVE SETS OF VARIABLES

We start this section with basic definitions and notation. A discrete function is defined as a mapping: $f : A \rightarrow B$ where the domain $A = \times_{i=1}^n A_i$ and range B are non-empty finite or countable sets.

To derive the means and methods to represent, and calculate with finite valued functions, some algebraic structure is imposed on the domain A and the range B . Both A and B throughout the present paper will be finite ring of integers.

Let $X = \{x_1, x_2, \dots\}$ be a countable set of variables and $X_n = \{x_1, x_2, \dots, x_n\}$ be a finite subset of X . Let $k, k \geq 2$ be a natural number and let us denote by $Z_k = \{0, 1, \dots, k-1\}$ the set (ring) of remainders modulo k . The set Z_k will identify the ring of residue classes *mod* k , i.e. $Z_k = \mathbb{Z}/_k\mathbb{Z}$, where \mathbb{Z} is the ring of all integers. An n -ary k -valued function (operation) on Z_k is a mapping $f : Z_k^n \rightarrow Z_k$ for some natural number n , called *the arity* of f . P_k^n denotes the set of all n -ary k -valued functions on Z_k . It is well known fact that there are k^{k^n} functions in P_k^n . The set of all k -valued functions $P_k = \bigcup_{n=1}^{\infty} P_k^n$ is called *the algebra of k -valued logic*.

All results obtained in the present paper can be easily extended to arbitrary algebra of finite operations.

For a given variable x and $\alpha \in Z_k$, x^α is defined as follows:

$$x^\alpha = \begin{cases} 1 & \text{if } x = \alpha \\ 0 & \text{if } x \neq \alpha. \end{cases}$$

We use *sums of products (SP)* to represent the functions from P_k^n . This is the most natural representation and it is based on so called operation tables of the functions. Thus each function $f \in P_k^n$ can be uniquely represented of SP-form as follows

$$f = a_0 \cdot x_1^0 \dots x_n^0 \oplus \dots \oplus a_m \cdot x_1^{\alpha_1} \dots x_n^{\alpha_n} \oplus \dots \oplus a_{k^n-1} \cdot x_1^{k-1} \dots x_n^{k-1}$$

with $\alpha = (\alpha_1, \dots, \alpha_n) \in Z_k^n$, where $m = \sum_{i=0}^n \alpha_i k^i \leq k^n - 1$. " \oplus " and " \cdot " denote the operations addition (sum) and multiplication (product) modulo k in the ring Z_k . Then (a_0, \dots, a_{k^n-1}) is the vector of output values of f in its table representation.

Let $f \in P_k^n$ and $\text{var}(f) = \{x_1, \dots, x_n\}$ be the set of all variables, which occur in f . We say that the i -th variable $x_i \in \text{var}(f)$ is *essential* in f , or f *essentially depends* on x_i , if there exist values $a_1, \dots, a_n, b \in Z_k$, such that

$$f(a_1, \dots, a_{i-1}, a_i, a_{i+1}, \dots, a_n) \neq f(a_1, \dots, a_{i-1}, b, a_{i+1}, \dots, a_n).$$

The set of all essential variables in the function f is denoted by $\text{Ess}(f)$ and the number of essential variables in f is denoted by $\text{ess}(f) = |\text{Ess}(f)|$. The variables from $\text{var}(f)$ which are not essential in f are called *inessential* or *fictive*.

The set of all output values of a function $f \in P_k^n$ is called *the range* of f , which is denoted as follows:

$$\text{range}(f) = \{c \in Z_k \mid \exists (a_1, \dots, a_n) \in Z_k^n, \text{ such that } f(a_1, \dots, a_n) = c\}.$$

Definition 2.1. Let x_i be an essential variable in f and $c \in Z_k$ be a constant from Z_k . The function $g = f(x_i = c)$ obtained from $f \in P_k^n$ by replacing the variable x_i with c is called a *simple subfunction* of f .

When g is a simple subfunction of f we shall write $g \prec f$. The transitive closure of \prec is denoted by \preceq . $Sub(f) = \{g \mid g \preceq f\}$ is the set of all subfunctions of f and $sub(f) = |Sub(f)|$.

For each $m = 0, 1, \dots, n$ we denote by $sub_m(f)$ the number of subfunctions in f with m essential variables, i.e. $sub_m(f) = |\{g \in Sub(f) \mid ess(g) = m\}|$.

Let $g \preceq f$, $\mathbf{c} = (c_1, \dots, c_m) \in Z_k^m$ and $M = \{x_1, \dots, x_m\} \subset X$ with

$$g \prec g_1 \prec \dots \prec g_m = f, \quad g = g_1(x_1 = c_1) \quad \text{and} \quad g_i = g_{i+1}(x_{i+1} = c_{i+1})$$

for $i = 1, \dots, m-1$. Then we shall write $g = f(x_1 = c_1, \dots, x_m = c_m)$ or equivalently, $g \preceq_M^{\mathbf{c}} f$ and we shall say that the vector \mathbf{c} determines the subfunction g in f .

Definition 2.2. Let M be a non-empty set of essential variables in the function f . Then M is called a separable set in f if there exists a subfunction g , $g \preceq f$ such that $M = Ess(g)$. $Sep(f)$ denotes the set of the all separable sets in f and $sep(f) = |Sep(f)|$.

The sets of essential variables in f which are not separable are called *inseparable* or *non-separable*.

For each $m = 1, \dots, n$ we denote by $sep_m(f)$ the number of separable sets in f which consist of m essential variables, i.e. $sep_m(f) = |\{M \in Sep(f) \mid |M| = m\}|$. The numbers $sub(f)$ and $sep(f)$ characterize the computational complexity of the function f when calculating its values. Our next goal is to classify the functions from P_k^n under these complexities. The initial and more fundamental results concerning essential variables and separable sets were obtained in the work of Y. Breitbart [2], K. Chimev [3], O. Lupanov [9], A. Salomaa [13], and others.

Remark 2.1. Note that if $g \preceq f$ and $x_i \notin Ess(f)$ then $x_i \notin Ess(g)$ and also if $M \notin Sep(f)$ then $M \notin Sep(g)$.

Definition 2.3. Let M and J be two non-empty sets of essential variables in the function f such that $M \cap J = \emptyset$. The set J is called a distributive set of M in f , if for every $|J|$ -tuple of constants \mathbf{c} from Z_k it holds $M \not\subseteq Ess(g)$, where $g \preceq_J^{\mathbf{c}} f$ and J is minimal with respect to the order \subseteq . $Dis(M, f)$ denotes the set of the all distributive sets of M in f .

It is clear that if $M \notin Sep(f)$ then $Dis(M, f) \neq \emptyset$. So, the distributive sets “dominate” on the inseparable sets of variables in a function. We are interested in the relationship between the structure of the distributive sets of variables and complexity of functions concerning $sep(f)$ and $sub(f)$, respectively, which is illustrated by the following example.

Example 2.1. Let $k = 2$, $f = x_1x_2 \oplus x_1x_3$ and $g = x_1x_2 \oplus x_1^0x_3$. It is easy to verify that the all three pairs of variables $\{x_1, x_2\}$, $\{x_1, x_3\}$ and $\{x_2, x_3\}$ are separable in f , but $\{x_2, x_3\}$ is inseparable in g . Figure 1 presents graphically, separable pairs in f and g . The set $\{x_1\}$ is distributive of $\{x_2, x_3\}$ in g .

Definition 2.4. Let $\mathcal{F} = \{P_1, \dots, P_m\}$ be a family of non-empty sets. A set $\beta = \{x_1, \dots, x_p\}$ is called an s -system of \mathcal{F} , if for all $P_i \in \mathcal{F}$, $1 \leq i \leq m$ there exists $x_j \in \beta$ such that $x_j \in P_i$ and for all $x_s \in \beta$ there exists $P_l \in \mathcal{F}$ such that $\{x_s\} = P_l \cap \beta$. $Sys(\mathcal{F})$ denotes the set of the all s -systems of the family \mathcal{F} .

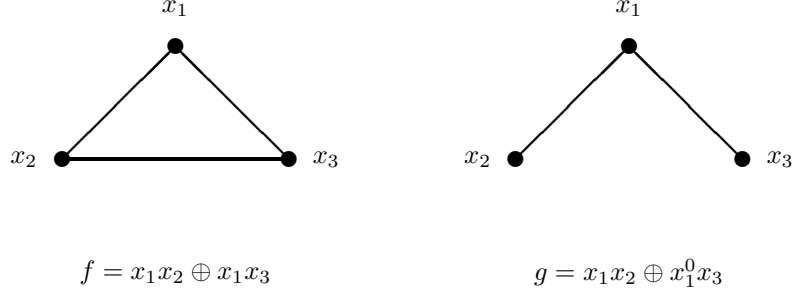


FIGURE 1. Separable pairs.

Applying the results concerning s -systems of distributive sets is one of the basic tools for studying inseparable pairs and inseparable sets in functions. These results are deeply discussed in [3, 14, 15].

Theorem 2.1. *Let $M \subseteq \text{Ess}(f)$ be a non-empty inseparable set of essential variables in $f \in P_k^n$ and $\beta \in \text{Sys}(\text{Dis}(M, f))$. Then the following statements hold:*

- (i) $M \cup \beta \in \text{Sep}(f)$;
- (ii) $(\forall \alpha, \alpha \subseteq \beta, \alpha \neq \beta) \quad M \cup \alpha \notin \text{Sep}(f)$.

Proof. (i) First, note that $M \notin \text{Sep}(f)$ implies $|M| \geq 2$. Without loss of generality assume that $\beta = \{x_1, \dots, x_m\} \in \text{Sys}(\text{Dis}(M, f))$ and $M = \{x_{m+1}, \dots, x_p\}$ with $1 \leq m < p \leq n$. Let us denote by L the following set of variables $L = \text{Ess}(f) \setminus (M \cup \beta) = \{x_{p+1}, \dots, x_n\}$.

Since $\beta \in \text{Sys}(\text{Dis}(M, f))$ it follows that for each $Q \subseteq L$ we have $Q \notin \text{Dis}(M, f)$. Hence there is a vector $\mathbf{c} = (c_{p+1}, \dots, c_n) \in Z_k^{n-p}$ such that $M \subseteq \text{Ess}(g)$ where $g \preceq_L^c f$.

Next, we shall prove that $\beta \subset \text{Ess}(g)$. For suppose this were not the case and without loss of generality, assume $x_1 \notin \text{Ess}(g)$, i.e. $g = g(x_1 = d_1)$ for each $d_1 \in Z_k$. Let $J \in \text{Dis}(M, f)$ be a distributive set of M such that $J \cap \beta = \{x_1\}$. The existence of the set J follows because β is an s -system of $\text{Dis}(M, f)$ (see Definition 2.4). Since $J \cap M = \emptyset$ and $x_1 \notin \text{Ess}(g)$ it follows that $J \cap \text{Ess}(g) = \emptyset$. Now $M \subset \text{Ess}(g)$ implies that $J \notin \text{Dis}(M, f)$, which is a contradiction. Thus we have $x_1 \in \text{Ess}(g)$ and $\beta \subset \text{Ess}(g)$. Then $\text{Ess}(f) \setminus L = M \cup \beta$ shows that $M \cup \beta = \text{Ess}(g)$ and hence $M \cup \beta \in \text{Sep}(f)$.

(ii) Let $\alpha, \alpha \subseteq \beta, \alpha \neq \beta$ be a proper subset of β . Let $x_i \in \beta \setminus \alpha$. Then $\beta \in \text{Sys}(\text{Dis}(M, f))$ implies that there is a distributive set $P \in \text{Dis}(M, f)$ of M such that $P \cap \beta = \{x_i\}$. Hence $P \cap \alpha = \emptyset$ which shows that there is a non-empty distributive set P_1 for $M \cup \{\alpha\}$ with $P_1 \subseteq P$. Hence $M \cup \alpha \notin \text{Sep}(f)$. \square

Corollary 2.1. *Let $\emptyset \neq M \subset \text{Ess}(f)$ and $M \notin \text{Sep}(f)$. If $\beta \in \text{Sys}(\text{Dis}(M, f))$ and $x_i \in \beta$ then $M \setminus \text{Ess}(f(x_i = c)) \neq \emptyset$ for all $c \in Z_k$.*

Theorem 2.2. [15] *For each finite family \mathcal{F} of non-empty sets there exists at least one s -system of \mathcal{F} .*

Theorem 2.3. *Let M be an inseparable set in f . A set $\beta \subset \text{Ess}(f)$ is an s -system of $\text{Dis}(M, f)$ if and only if $\beta \cap J \neq \emptyset$ for all $J \in \text{Dis}(M, f)$ and $\alpha \subseteq \beta, \alpha \neq \beta$ implies $\alpha \cap P = \emptyset$ for some $P \in \text{Dis}(M, f)$.*

Proof. " \Leftarrow " Let $\beta \cap J \neq \emptyset$ for all $J \in \text{Dis}(M, f)$ and $\alpha \subsetneq \beta$ implies $\alpha \cap P = \emptyset$ for some $P \in \text{Dis}(M, f)$. Since $\beta \cap J \neq \emptyset$ it follows that there is a set β' , $\beta' \subset \beta \subset \text{Ess}(f)$ and $\beta' \in \text{Sys}(\text{Dis}(M, f))$. If we suppose that $\beta' \neq \beta$ then there is $P \in \text{Dis}(M, f)$ with $\beta' \cap P = \emptyset$. Hence $M \cup \beta' \notin \text{Sep}(f)$ because of $P \in \text{Dis}(M \cup \beta', f)$ which contradicts Theorem 2.1.

" \Rightarrow " Let β be an s -system of $\text{Dis}(M, f)$ and $\alpha \subsetneq \beta$. Let $x \in \beta \setminus \alpha$ and $P \in \text{Dis}(M, f)$ be a distributive set of M for which $\beta \cap P = \{x\}$. Hence $\alpha \cap P = \emptyset$ and we have $P \in \text{Dis}(M \cup \alpha, f)$ and $M \cup \alpha \notin \text{Sep}(f)$ which shows that $\alpha \notin \text{Sys}(\text{Dis}(M, f))$. \square

3. ORDERED DECISION DIAGRAMS AND COMPLEXITY OF FUNCTIONS

The distributive sets are also important when constructing efficient procedures for simplifying in analysis and synthesis of functional schemas.

In this section we discuss *ordered decision diagrams* (ODDs) for the functions obtained by restrictions on their *ordered decomposition trees* (ODTs).

Figure 2 shows an ordered decomposition tree for the function $g = x_1x_2 \oplus x_1^0x_3 \in P_2^3$ from Example 2.1, which essentially depends on all its three variables x_1, x_2 and x_3 . The node at the top, labelled g - is the *function* node. The nodes drawn as filled circles labelled with variable names are the *internal (non-terminal)* nodes, and the rectangular nodes (leaves of the tree) are the *terminal* nodes. The terminal nodes are labelled by the numbers from Z_k . Implementation of g for a given values of x_1, x_2 and x_3 consists of selecting a path from the function node to a terminal node. The label of the terminal node is the sought value. At each non-terminal node the path follows the solid edge if the variable labelling the node evaluates to 1, and the dashed edge if the variable evaluates to 0. In the case of $k > 2$ we can use colored edges with k distinct colors.

The ordering in which the variables appear is the same along all paths of an ODT. Figure 2 shows the ODT for the function g from Example 2.1, corresponding to the variable ordering x_1, x_2, x_3 (denoted briefly as $\langle 1; 2; 3 \rangle$). It is known that for a given function g and a given ordering of its essential variables there is a unique ODT.

We extend our study to ordered decision diagrams for the functions from P_k^n which were studied by D. Miller and R. Drechsler [10, 11].

An *ordered decision diagram* of a function f is obtained from the corresponding ODT by *reduction* of its nodes applying of the following two rules starting from the ODT and continuing until neither rule can be applied:

Reduction rules

- If two nodes are terminal and have the same label, or are non-terminal and have the same children, they are merged.
- If a non-terminal node has identical children it is removed from the graph and its incoming edges are redirected to the child.

When $k = 2$ ODD is called a *binary decision diagram* (BDD). BDDs are extensively used in the theory of *switching circuits* to represent and manipulate Boolean functions and to measure the complexity of binary terms.

The size of the ODD is determined both by the function being represented and the chosen ordering of the variables. It is of crucial importance to care about variable ordering when applying ODDs in practice. The problem of finding the best variable ordering is NP-complete (see [1]).

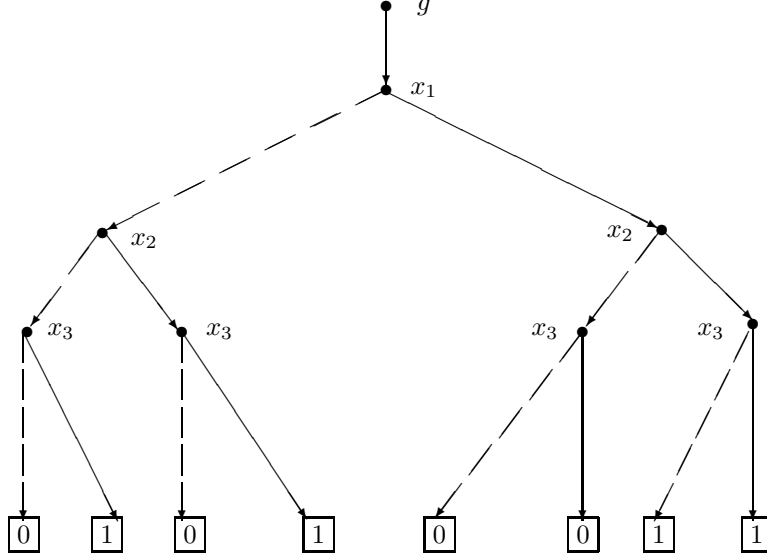
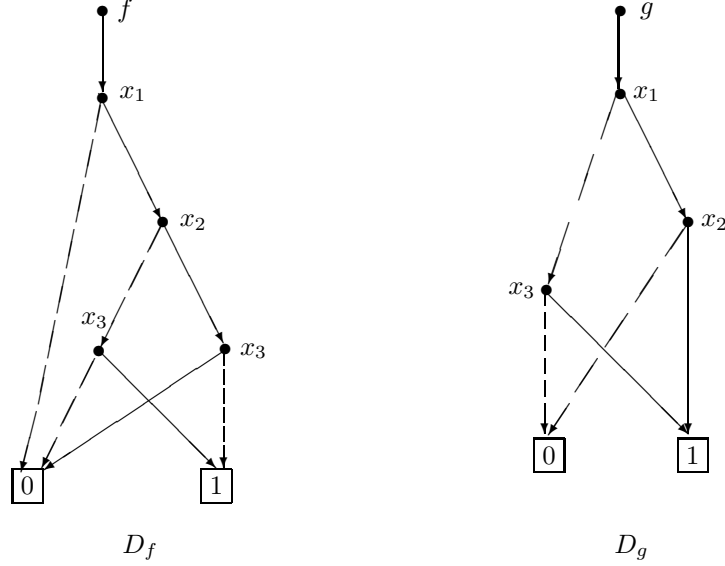
FIGURE 2. Decomposition tree for $g = x_1x_2 \oplus x_1^0x_3$.FIGURE 3. BDD for f and g under the natural ordering of variables.

Figure 3 shows the BDDs for the functions from Example 2.1 obtained from their decomposition trees under the natural ordering of their variables - $\langle 1; 2; 3 \rangle$. The construction of the ODT for f under the natural ordering of the variables is left to the reader.

The BDD of f is more complex than the BDD of g . This reflects the fact that f has more separable pairs. Thus we have $M = \{x_2, x_3\} \notin \text{Sep}(g)$, $\{x_1\} \in \text{Dis}(M, g)$

and $\{x_1\} \in Sys(Dis(M, g))$. Additionally, the diagram of g starts with x_1 - a variable which belongs to an s -system of $Dis(M, g)$. In this simple case we have $Sys(Dis(M, g)) = Dis(M, g) = \{x_1\}$.

Figure 3 shows that when constructing the ODD of a function, it is better to start with the variables from an s -system of the family of distributive sets of an inseparable set M in this function. In [5] it is shown that the BDDs of functions have to be most simple when starting with variables from $Sys(Dis(M, f))$. Consequently, the inseparable sets with their distributive sets are important in theoretical and applied computer science concerning the computational complexity of the functions.

Next, we define and explore complexity measures of the functions in P_k^n which are directly connected with the computational complexity of functions. We might think that the complexity of a function f depends on the complexity of its ODDs.

Let $f \in P_k^n$ and let $DD(f)$ be the set of the all ODDs for f constructed under different variable orderings in f .

Definition 3.1. *Each path starting from the function node and finishing into a terminal node is called an implementation of the function f under the given variable ordering. The set of the all implementations of D_f we denote by $Imp(D_f)$ and*

$$Imp(f) = \bigcup_{D_f \in DD(f)} Imp(D_f).$$

Each implementation of the function $f \in P_k^n$, obtained from the diagram D_f of f by the non-terminal nodes x_{i_1}, \dots, x_{i_r} and corresponding constants $c_1, \dots, c_r, c \in Z_k$ with $f(x_{i_1} = c_1, \dots, x_{i_r} = c_r) = c$, $r \leq ess(f)$, can be represented as a pair (\mathbf{i}, \mathbf{c}) of two words (strings) over $\mathbf{n} = \{1, \dots, n\}$ and Z_k where $\mathbf{i} = i_1 i_2 \dots i_r \in \mathbf{n}^*$ and $\mathbf{c} = c_1 c_2 \dots c_r c \in Z_k^*$.

There is an obvious way to define a measure of complexity of a given ordered decision diagram D_f , namely as the number $imp(D_f)$ of all paths in D_f which starts from the function node and finish in a terminal node of the diagram.

The *implementation complexity* of a function $f \in P_k^n$ is defined as the number of all implementations of f , i.e. $imp(f) = |Imp(f)|$.

We shall study also two other measures of computational complexity of functions as $sub(f)$ and $sep(f)$.

Example 3.1. *Let us consider again the functions f and g from Example 2.1, namely $f = x_1 x_2 \oplus x_1 x_3$ and $g = x_1 x_2 \oplus x_1^0 x_3$.*

Then $(123, 1011)$ is an implementation of f obtained by the diagram D_f presented in Figure 3, following the path $\pi = (f; x_1 : 1; x_2 : 0; x_3 : 1; \text{terminal node} : 1)$.

It is easy to see that there are six distinct BDDs for f and five distinct BDDs for g . We shall calculate the implementations of f and g for the variable orderings $\langle 1; 2; 3 \rangle$ (see Figure 3) and $\langle 2; 1; 3 \rangle$, only. Thus for f we have:

ordering	implementations
$\langle 1; 2; 3 \rangle$	$(1, 00); (123, 1000); (123, 1011); (123, 1101); (123, 1110)$
$\langle 2; 1; 3 \rangle$	$(21, 000); (213, 0100); (213, 0111); (21, 100); (213, 1101); (213, 1110)$

For the function g we obtain:

ordering	implementations
$\langle 1; 2; 3 \rangle$	$(13, 000); (13, 011); (12, 100); (12, 111)$
$\langle 2; 1; 3 \rangle$	$(21, 010); (213, 0000); (213, 0011); (213, 1000); (213, 1011); (21, 111)$

For the diagrams in Figure 3 we have $\text{imp}(D_f) = 5$ and $\text{imp}(D_g) = 4$.

Since f is a symmetric function with respect to x_2 and x_3 one can count that $\text{imp}(f) = 33$. Note that the implementation $(1, 00)$ occurs in two distinct diagrams of f , namely under the orderings $\langle 1; 2; 3 \rangle$ and $\langle 1; 3; 2 \rangle$. Hence, it has to be counted one time and we obtain that $\text{imp}(f)$ is equal to 33 instead of 34.

For the function g , the diagrams under the orderings $\langle 1; 2; 3 \rangle$ and $\langle 1; 3; 2 \rangle$ have the same implementations, i.e. the diagrams are identical (isomorphic). This fact is a consequence of inseparability of the set $\{x_2, x_3\}$. Hence g has five (instead of six for f) distinct ordered decision diagrams. Then, one might calculate that $\text{imp}(g) = 28$.

For the other two measures of complexity we obtain: $\text{sub}(f) = 13$ because of $\text{Sub}(f) = \{0, 1, x_1, x_2, x_3, x_2^0, x_3^0, x_2 \oplus x_3, x_1 x_2, x_1 x_2^0, x_1 x_3, x_1 x_3^0, f\}$ and $\text{sub}(g) = 11$ because of $\text{Sub}(g) = \{0, 1, x_1, x_2, x_3, x_1^0, x_1 x_2, x_1^0 x_3, x_1 \oplus x_1^0 x_3, x_1 x_2 \oplus x_1^0, g\}$. Furthermore, $\text{sep}(f) = 7$ because of $M \in \text{Sep}(f)$ for all M , $\emptyset \neq M \subseteq \{x_1, x_2, x_3\}$ and $\text{sep}(g) = 6$ because of $\text{Sep}(g) = \{\{x_1\}, \{x_2\}, \{x_3\}, \{x_1, x_2\}, \{x_1, x_3\}, \{x_1, x_2, x_3\}\}$.

Lemma 3.1. *A variable x_i is essential in $f \in P_k^n$ if and only if x_i occurs as a label of an non-terminal node in any ODD of f .*

Proof. " \Rightarrow " Let us assume that x_i does not occur as a label of any non-terminal node in an ordered decision diagram D_f of f . Since all values of the function f can be obtained by traversal walk-through all paths in D_f from function node to leaf nodes this will mean that x_i will not affect the function value and hence x_i is an inessential variable in f .

" \Leftarrow " Let $x_i \notin \text{Ess}(f)$ be an inessential variable in f . It is obvious that for each subfunction g of f we have $x_i \notin \text{Ess}(g)$. Then we have $f(x_i = c) = f(x_i = d)$ for all $c, d \in Z_k$. Consequently, if there is a non-terminal node labelled by x_i in an ODT of f then its children have to be identical, which shows that this node has to be removed from the ODT, according to the reduction rules, given above. \square

An essential variable x_i in a function f is called a *strongly essential variable* in f if there is a constant $c \in Z_k$ such that $\text{Ess}(f(x_i = c)) = \text{Ess}(f) \setminus \{x_i\}$.

Fact 3.1. *If $\text{ess}(f) \geq 1$ then there is at least one strongly essential variable in f .*

This fact was proven by O. Lupanov [9] in case of Boolean functions and by A. Salomaa [13] for arbitrary functions. Later, Y. Breitbart [2] and K. Chimev [3] proved that if $\text{ess}(f) \geq 2$ then there exist at least two strongly essential variables in f . We need Fact 3.1 to prove the next important theorem.

Theorem 3.1. *A non-empty set M of essential variables is separable in f if and only if there exists an implementation (\mathbf{j}, \mathbf{c}) of the form*

$$(\mathbf{j}, \mathbf{c}) = (j_1 j_2 \dots j_{r-m} j_{r-m+1} \dots j_r, c_1 c_2 \dots c_{r-m} c_{r-m+1} \dots c_r c) \in \text{Imp}(f)$$

where $M = \{x_{j_{r-m+1}}, \dots, x_{j_r}\}$ and $1 \leq m \leq r \leq \text{ess}(f)$.

Proof. " \Leftarrow " Let

$$(\mathbf{j}, \mathbf{c}) = (j_1 \dots j_{r-m} j_{r-m+1} \dots j_r, c_1 \dots c_{r-m} c_{r-m+1} \dots c_r c) \in \text{Imp}(f)$$

be an implementation of f and let $M = \{x_{j_{r-m+1}}, \dots, x_{j_r}\}$. Hence the all variables from $\{x_{j_{r-m+1}}, \dots, x_{j_r}\}$ are essential in the following subfunction of f

$$g = f(x_{j_1} = c_1, \dots, x_{j_{r-m}} = c_{r-m})$$

which shows that $M \in \text{Sep}(f)$.

" \Rightarrow " Without loss of generality let us assume that $M = \{x_1, \dots, x_m\}$ is a non-empty separable set in f and $n = \text{ess}(f)$. Then there are constants $d_{m+1}, \dots, d_n \in Z_k$ such that $M = \text{Ess}(h)$ where $h = f(x_{m+1} = d_{m+1}, \dots, x_n = d_n)$. From Fact 3.1 it follows that there is a variable $x_{i_1} \in M$ and a constant $d_1 \in Z_k$ such that $\text{Ess}(h_1) = M \setminus \{x_{i_1}\}$ where $h_1 = h(x_{i_1} = d_1)$. Consequently, we might inductively obtain that there are variables $x_{i_r} \in M$ and constants $d_r \in Z_k$ for $r = 2, \dots, m$, such that $\text{Ess}(h_r) = M \setminus \{x_{i_1}, \dots, x_{i_r}\}$ where $h_r = h_{r-1}(x_{i_r} = d_r)$. Hence, the string $m+1m+2 \dots n$ has a substring $j_1 \dots j_s$ such that $(j_1 \dots j_s i_1 \dots i_m, d_{j_1} \dots d_{j_s} d_1 \dots d_m d)$ is an implementation of f with $M = \{x_{i_1}, \dots, x_{i_m}\}$ and $d = h_m$. \square

Corollary 3.1. *For each variable $x_i \in \text{Ess}(f)$ there is an implementation (\mathbf{j}, \mathbf{c}) of f whose last letter of \mathbf{j} is i , i.e. $(\mathbf{j}, \mathbf{c}) = (j_1 \dots j_{m-1} i, c_{j_1} \dots c_{j_{m-1}} c_i c) \in \text{Imp}(f)$, $m \leq \text{ess}(f)$.*

Note that there exists an ODD of a function whose non-terminal nodes are labelled by the variables from a given set, but this set might not be separable. For instance, the implementation $(231, 0101) \in \text{Imp}(g)$ of the function g from Example 3.1 shows that the variables from the set $M = \{x_2, x_3\}$ occur as labels of the starting two non-terminal nodes in the BDD of g under the ordering $\langle 2; 3; 1 \rangle$, but $M \notin \text{Sep}(g)$.

Lemma 3.2. *If $\text{ess}(f) = n$, $g \preceq f$ with $\text{ess}(g) = m < n$ then there exists a variable $x_t \in \text{Ess}(f) \setminus \text{Ess}(g)$ such that $\text{Ess}(g) \cup \{x_t\} \in \text{Sep}(f)$.*

Proof. Let $M = \text{Ess}(g)$. Then $M \in \text{Sep}(f)$ and from Theorem 3.1 it follows that there is an implementation (\mathbf{j}, \mathbf{c}) of the form $(\mathbf{j}, \mathbf{c}) = (j_1 j_2 \dots j_{r-m} j_{r-m+1} \dots j_r, c_1 c_2 \dots c_{r-m} c_{r-m+1} \dots c_r c) \in \text{Imp}(f)$ where $M = \{x_{j_{r-m+1}}, \dots, x_{j_r}\}$ and $1 \leq m \leq r \leq \text{ess}(f)$. Since $m < n$ it follows that $r - m > 0$ and Lemma 3.1 shows that there is $x_{j_i} \in \text{Ess}(h)$ where

$$h = f(x_{j_1} = c_1, \dots, x_{j_{i-1}} = c_{i-1}, x_{j_{i+1}} = c_{i+1}, \dots, x_{j_{r-m}} = c_{r-m}).$$

It is easy to see that $\text{Ess}(h) = M \cup \{x_{j_i}\}$. \square

Now, as an immediate consequence of the above lemma we obtain Theorem 3.2 which was inductively proven by K. Chimev.

Theorem 3.2. [3] *If $\text{ess}(f) = n$, $g \preceq f$ with $\text{ess}(g) = m \leq n$ then there exist $n - m$ subfunctions g_1, \dots, g_{n-m} such that*

$$g \prec g_1 \prec g_2 \prec \dots \prec g_{n-m} = f$$

and $\text{ess}(g_i) = m + i$ for $i = 1, \dots, n - m$.

The *depth*, (denoted by $\text{Depth}(D_f)$) of an ordered decision diagram D_f for a function f is defined as the number of the edges in a longest path from the function node in D_f to a leaf of D_f .

Thus for the diagrams in Figure 3 we have $\text{Depth}(D_f) = 4$ and $\text{Depth}(D_g) = 3$.

Clearly, if $\text{ess}(f) = n$ then $\text{Depth}(D_f) \leq n + 1$ for all ODDs of f .

Theorem 3.3. *If $\text{ess}(f) = n \geq 1$ then there is an ordered decision diagram D_f of f with $\text{Depth}(D_f) = n + 1$.*

Proof. Let $Ess(f) = \{x_1, \dots, x_n\}$, $n \geq 1$. Since x_1 is an essential variable it follows that $\{x_1\} \in Sep(f)$. Theorem 3.2 implies that there is an ordering $\langle i_1; i_2; \dots; i_{n-1} \rangle$ of the rest variables x_2, \dots, x_n such that for each j , $1 \leq j \leq n-1$ we have $g_j \prec_J^c f$ where $J = \{x_{i_1}, \dots, x_{i_j}\}$, $c \in Z_k^J$ and $Ess(g_j) = \{x_1, x_{i_{j+1}}, \dots, x_{i_{n-1}}\}$. This shows that the all variables from J have to be labels of non-terminal nodes in a path π of the ordered decision diagram D_f of f under the variable ordering $\langle i_1; i_2; \dots; i_{n-1}; 1 \rangle$. Hence π has to contain all essential variables in f as labels at the non-terminal nodes of π . Hence $Depth(D_f) = n + 1$. \square

Theorem 3.4. *Let $f \in P_k^n$ and $Ess(f) = \{x_1, \dots, x_n\}$, $n \geq 1$. If $M \neq \emptyset$, $M \subset Ess(f)$ and $M \notin Sep(f)$ then there is a decision diagram D_f of f with $Depth(D_f) < n + 1$.*

Proof. Without loss of generality, let us assume that $M = \{x_1, \dots, x_m\}$, $m < n$. Since M is inseparable in f , the family $Dis(M, f)$ of the all distributive sets of M is non-empty. According to Theorem 2.2 there is a non-empty s -system $\beta = \{x_{i_1}, \dots, x_{i_t}\}$ of $Dis(M, f)$. Since $f(x_{i_1} = c_1) \neq f(x_{i_1} = c_2)$ for some $c_1, c_2 \in Z_k$ it follows that there exists an ODD D_f for f under a variable ordering with x_{i_1} as the label of the first non-terminal node of D_f . According to Corollary 2.1 for all $c \in Z_k$ there is a variable $x_j \in M$ which is inessential in $f(x_{i_1} = c)$. Hence, each path of D_f does not contain at least one variable from M among its labels of non-terminal nodes. Hence $Depth(D_f) < n + 1$. \square

4. EQUIVALENCE RELATIONS AND TRANSFORMATION GROUPS IN P_k^n

Many of the problems in applications of the k -valued functions are compounded because of the large number of the functions, namely k^{k^n} . Techniques which involve enumeration of functions can only be used if k and n are trivially small. A common way for extending the scope of such enumerative methods is to classify the functions into equivalence classes under some natural equivalence relation.

In this section we define equivalence relations in P_k^n which classify functions with respect to number of their implementations, subfunctions and separable sets. We are intended to determine several numerical invariants of the transformation groups generated by these relations. The second goal is to compare these groups with so called classical subgroups of the Restricted Affine Group(RAG) [7] which have a variety of applications such as coding theory, switching theory, multiple output combinational logic, sequential machines and other areas of theoretical and applied computer sciences.

Let us denote by S_A the symmetric group of all permutations of a given non-empty set A . S_m denotes the symmetric group $S_{\{1, \dots, m\}}$ for a natural number m , $m \geq 1$.

Let us define the following three equivalence relations: \simeq_{imp} , \simeq_{sub} and \simeq_{sep} .

Definition 4.1. *Let $f, g \in P_k^n$ be two functions.*

- (i) *If $ess(f) = ess(g) \leq 1$ then $f \simeq_{imp} g$;*
- (ii) *Let $ess(f) = n > 1$. We say that f is imp-equivalent to g (written $f \simeq_{imp} g$) if there are $\pi \in S_n$ and $\sigma_i \in S_{Z_k}$ such that $f(x_i = j) \simeq_{imp} g(x_{\pi(i)} = \sigma_i(j))$ for all $i = 1, \dots, n$ and $j \in Z_k$.*

Hence two functions are *imp*-equivalent if they produce same number of implementations, i.e. $imp(f) = imp(g)$ and there are $\pi \in S_n$, and $\sigma_i \in S_{Z_k}$ such that

$$(i_1 \dots i_m, c_1, \dots, c_m c) \in \text{Imp}(f) \iff (\pi(i_1) \dots \pi(i_m), \sigma_1(c_1) \dots \sigma_m(c_m) \sigma(c)) \in \text{Imp}(g).$$

Table 1 shows the classification of Boolean functions of two variables into four classes, called *imp-classes* under the equivalence relation \simeq_{imp} . The second column shows the number of implementations of the functions from the *imp-classes* given at the first column. The third column presents the number of functions per each *imp-class*.

TABLE 1. *Imp-classes* in P_2^2 .

$[0, 1]$	1	2
$[x_1, x_2, x_1^0, x_2^0]$	2	4
$[x_1 x_2, x_1 x_2^0, x_1^0 x_2, x_1^0 x_2^0, x_1 \oplus x_1 x_2, x_2^0 \oplus x_1 x_2, x_1^0 \oplus x_1 x_2, x_1^0 \oplus x_1 x_2^0]$	6	8
$[x_1 \oplus x_2, x_1 \oplus x_2^0]$	8	2

Definition 4.2. Let $f, g \in P_k^n$ be two functions.

- (i) If $\text{ess}(f) = \text{ess}(g) = 0$ then $f \simeq_{\text{sub}} g$;
- (ii) If $\text{ess}(f) = \text{ess}(g) = 1$ then $f \simeq_{\text{sub}} g \iff \text{range}(f) = \text{range}(g)$;
- (iii) Let $\text{ess}(f) = n > 1$. We say that f is sub-equivalent to g (written $f \simeq_{\text{sub}} g$) if $\text{sub}_m(f) = \text{sub}_m(g)$ for all $m = 0, 1, \dots, n$.

It is easy to see that the equivalence relation \simeq_{sub} partitions the algebra of Boolean functions of two variables in the same equivalence classes (called *the sub-classes*) as the relation \simeq_{imp} (see Table 1).

Definition 4.3. Let $f, g \in P_k^n$ be two functions.

- (i) If $\text{ess}(f) = \text{ess}(g) \leq 1$ then $f \simeq_{\text{sep}} g$;
- (ii) Let $\text{ess}(f) = n > 1$. We say that f is sep-equivalent to g (written $f \simeq_{\text{sep}} g$) if $\text{sep}_m(f) = \text{sep}_m(g)$ for all $m = 1, \dots, n$.

The equivalence classes under \simeq_{sep} are called *sep-classes*.

Since P_k^n is a finite algebra of k -valued functions each equivalence relation \simeq on P_k^n makes a partition of the algebra in the set of disjoint equivalence classes $Cl(\simeq) = \{P_1^\simeq, \dots, P_r^\simeq\}$. Then, in the set of all equivalence relations a partial order is defined as follows: $\simeq_1 \leq \simeq_2$ if for each $P \in Cl(\simeq_1)$ there is a $Q \in Cl(\simeq_2)$ such that $P \subseteq Q$. Thus $\simeq_1 \leq \simeq_2$ if and only if $f \simeq_1 g \Rightarrow f \simeq_2 g$, for $f, g \in P_k^n$.

Theorem 4.1.

- (i) $\simeq_{\text{imp}} \leq \simeq_{\text{sep}}$; (iii) $\simeq_{\text{imp}} \not\leq \simeq_{\text{sub}}$;
- (ii) $\simeq_{\text{sub}} \leq \simeq_{\text{sep}}$; (iv) $\simeq_{\text{sub}} \not\leq \simeq_{\text{imp}}$.

Proof. (i) Let $f, g \in P_k^n$ be two *imp*-equivalent functions, i.e. $f \simeq_{\text{imp}} g$. We shall proceed by induction on the number $n = \text{ess}(f)$ of essential variables in f and g .

Clearly, if $n \leq 1$ then $f \simeq_{\text{sub}} g$, which is our inductive basis. Let us assume that $f \simeq_{\text{imp}} g$ implies $f \simeq_{\text{sep}} g$ if $n < r$ for some natural number r , $r \geq 2$.

Let f and g be two functions with $f \simeq_{\text{imp}} g$ and $\text{ess}(f) = \text{ess}(g) = r$. Then there are $\pi \in S_r$ and $\sigma_i \in S_{Z_k}$ for $i = 1, \dots, r$ such that $f(x_i = j) \simeq_{\text{imp}} g(x_{\pi(i)} = \sigma_i(j))$.

Let $M, \emptyset \neq M \in \text{Sep}(f)$ be a separable set of essential variables in f with $|M| = m$, $1 \leq m \leq r$. Theorem 3.1 implies that there is an implementation

$$(\mathbf{j}, \mathbf{c}) = (j_1 \dots j_{r-m} i_1 \dots i_m, c_{j_1} \dots c_{j_{r-m}} c_{i_1} \dots c_{i_m} c)$$

of f obtained under an ODD whose variable ordering finishes with the variables from M , i.e. $M = \{x_{i_1}, \dots, x_{i_m}\}$. Then $f(x_{j_1} = c_{j_1}) \simeq_{\text{imp}} g(x_{\pi(j_1)} = \sigma_{j_1}(c_{j_1}))$ implies that

$$(\pi(j_1) \dots \pi(j_{r-m}) \pi(i_1) \dots \pi(i_m), \sigma_{j_1}(c_{j_1}) \dots \sigma_{j_{r-m}}(c_{j_{r-m}}) \sigma_{i_1}(c_{i_1}) \dots \sigma_{i_m}(c_{i_m}) \sigma(c))$$

is an implementation of g , for some $\sigma \in S_{Z_k}$. Again, from Theorem 3.1 it follows that $\pi(M) = \{x_{\pi(i_1)}, \dots, x_{\pi(i_m)}\} \in \text{Sep}(g)$. Since π is a permutation of S_r it follows that $\text{sep}_m(f) = \text{sep}_m(g)$ for $m = 1, \dots, r$ and hence $\simeq_{\text{imp}} \leq \simeq_{\text{sep}}$.

(ii) Definition 2.2 shows that $M \in \text{Sep}(f)$ if and only if there is a subfunction $g \in \text{Sub}(f)$ with $g \prec_Q^c f$ where $Q = \text{Ess}(f) \setminus M$ and $\mathbf{c} \in Z_k^{n-|M|}$. Hence

$$\forall f, g \in P_k^n, \quad \text{Sub}(f) = \text{Sub}(g) \implies \text{Sep}(f) = \text{Sep}(g),$$

which implies that $\text{sub}_m(f) = \text{sub}_m(g) \implies \text{sep}_m(f) = \text{sep}_m(g)$ and $\simeq_{\text{sub}} \leq \simeq_{\text{sep}}$.

(iii) Let us consider the functions

$$f = x_1^0 x_2 x_3 \oplus x_1 x_2^0 x_3^0 \pmod{2} \quad \text{and} \quad g = x_2 x_3 \oplus x_1 x_2^0 x_3 \oplus x_1 x_2 x_3^0 \pmod{2}.$$

The set of the all simple subfunctions in f is: $\{x_1 x_2^0, x_1^0 x_2, x_1 x_3^0, x_1^0 x_3, x_2 x_3, x_2^0 x_3^0\}$ and in g is: $\{x_1 x_2, x_1 x_3, x_2 x_3, x_2 \oplus x_1 x_2^0, x_3 \oplus x_1 x_3^0, x_2^0 x_3^0 \oplus 1\}$.

Hence f and g have six simple subfunctions, which depends essentially on two variables. Table 1 shows that all these subfunctions belong to same *imp*-class and the number of their implementations is 6. Thus we might calculate that $\text{imp}(f) = \text{imp}(g) = 36$ and $f \simeq_{\text{imp}} g$.

The set of the all subfunctions with one essential variable in the function f is: $\{x_1, x_2, x_3, x_1^0, x_2^0, x_3^0\}$ and in g is: $\{x_1, x_2, x_3\}$.

Then we have $\text{sub}_0(f) = \text{sub}_0(g) = 2$, $\text{sub}_1(f) = 6$, $\text{sub}_1(g) = 3$ and $\text{sub}_2(f) = \text{sub}_2(g) = 6$ and hence $f \not\simeq_{\text{sub}} g$. It is clear that $\text{sub}(f) = 15$, $\text{sub}(g) = 12$ and $\simeq_{\text{imp}} \not\leq \simeq_{\text{sub}}$.

(iv) Let us consider the functions

$$f = x_1 x_2^0 x_3^0 \oplus x_1 \pmod{2} \quad \text{and} \quad g = x_1 x_2 x_3 \pmod{2}.$$

The simple subfunctions in f and g are:

$$\begin{array}{lll} f(x_1 = 0) = 0, & f(x_3 = 0) = x_1 x_2^0 \oplus x_1, & g(x_2 = 0) = 0, \\ f(x_1 = 1) = x_2^0 x_3^0 \oplus 1, & f(x_3 = 1) = x_1, & g(x_2 = 1) = x_1 x_3, \\ f(x_2 = 0) = x_1 x_3^0 \oplus x_1, & g(x_1 = 0) = 0, & g(x_3 = 0) = 0, \\ f(x_2 = 1) = x_1, & g(x_1 = 1) = x_2 x_3, & g(x_3 = 1) = x_1 x_2. \end{array}$$

Now, using Table 1, one can easily calculate that $\text{imp}(f) = 23$ and $\text{imp}(g) = 21$, and hence $f \not\simeq_{\text{imp}} g$. On the other side we have $\text{Sub}(f) = \{0, 1, x_1, x_2, x_3, x_2^0 x_3^0 \oplus 1, x_1 x_3^0 \oplus x_1, x_1 x_2^0 \oplus x_1, f\}$ and $\text{Sub}(g) = \{0, 1, x_1, x_2, x_3, x_2 x_3, x_1 x_3, x_1 x_2, g\}$ which show that $\text{sub}_m(f) = \text{sub}_m(g)$ for $m = 0, 1, 2, 3$ and $f \simeq_{\text{sub}} g$. Hence $\simeq_{\text{sub}} \not\leq \simeq_{\text{imp}}$. \square

A transformation $\psi : P_k^n \longrightarrow P_k^n$ can be viewed as an n -tuple of functions

$$\psi = (g_1, \dots, g_n), \quad g_i \in P_k^n, \quad i = 1, \dots, n$$

acting on any function $f = f(x_1, \dots, x_n) \in P_k^n$ as follows $\psi(f) = f(g_1, \dots, g_n)$. Then the composition of two transformations ψ and $\phi = (h_1, \dots, h_n)$ is defined as follows

$$\psi\phi = (h_1(g_1, \dots, g_n), \dots, h_n(g_1, \dots, g_n)).$$

Thus the set of all transformations of P_k^n is the *universal monoid* Ω_k^n with unity - the identical transformation. When taking only invertible transformations we obtain the *universal group* C_k^n isomorphic to the symmetric group $S_{Z_k^n}$. Throughout this paper we shall consider invertible transformation, only. The groups consisting of invertible transformations of P_k^n are called *transformation groups*.

Let \simeq be an equivalence relation in P_k^n . A mapping $\varphi : P_k^n \rightarrow P_k^n$ is called a *transformation, preserving* \simeq if $f \simeq \varphi(f)$ for all $f \in P_k^n$. Taking only invertible transformations which preserve \simeq , we get the group G of all transformations preserving \simeq , whose *orbits* (also called *G-types*) are the equivalence classes P_1, \dots, P_r under \simeq . The number of orbits of a group G of transformations in finite algebras of functions is denoted by $t(G)$.

Next, we relate groups to combinatorial problems through the following obvious, but important definition:

Definition 4.4. Let G be a transformation group acting on the algebra of functions P_k^n and suppose that $f, g \in P_k^n$. We say that f is G -equivalent to g (written $f \simeq_G g$) if there exists $\psi \in G$ so that $g = \psi(f)$.

Clearly, the relation \simeq_G is an equivalence relation. We summarize and extend the results for the "classical" transformation groups, following [6, 7, 16], where these notions are used to study classification and enumeration in the algebra of boolean functions. Such groups are induced under the following notions of equivalence: complementation and/or permutation of the variables; any linear or affine function of the variables. Since we want to classify functions from P_k^n into equivalence classes, three natural problems occur.

- We ask for the number $t(G)$ of such equivalence classes. This problem will be partially discussed for the family of "natural" equivalence relations in the algebra of boolean functions.
- We ask for the cardinalities of the equivalence classes. This problem is important in applications as functioning the switching gates, circuits etc. For boolean functions of 3 and 4 variables we shall solve these two problems, also concerning *imp*-, *sub*- and *sep*-classes.
- We want to give a method which will decide the class to which an arbitrary function belongs. In some particular cases this problem will be discussed below. We also develop a class of algorithms for counting the complexities *imp*, *sub* and *sep* for each boolean function which allow us to classify the algebras P_2^n for $n = 2, 3, 4$ with respect to these complexities as group invariants.

These problems are very hard and for $n \geq 5$ they are practically unsolvable.

We use the denotation \leq also, for order relation "subgroup". More precisely, $H \leq G$ if there is a subgroup G' of G which is isomorphic to H .

Let us denote by IM_k^n , SB_k^n and SP_k^n the transformation groups induced by the equivalence relations \simeq_{imp} , \simeq_{sub} and \simeq_{sep} , respectively.

Now, as a direct consequence of Theorem 4.1 we obtain the following proposition.

Proposition 4.1.

$$\begin{aligned} (i) \quad & IM_k^n \leq SP_k^n; & (iii) \quad & IM_k^n \not\leq SB_k^n; \\ (ii) \quad & SB_k^n \leq SP_k^n; & (iv) \quad & SB_k^n \not\leq IM_k^n. \end{aligned}$$

We deal with "natural" equivalence relations which involve variables in some functions. Such relations induce permutations on the domain Z_k^n of the functions. These mappings form a transformation group whose number of equivalence classes can be determined.

The restricted affine group (RAG) is defined as a subgroup of the symmetric group on the direct sum of the vector space Z_k^n of arguments of functions and the vector space Z_k of their outputs. The group RAG permutes the direct sum $Z_k^n + Z_k$ under restrictions which preserve single-valuedness of all functions from P_k^n . The equivalence relation induced by RAG is called *prototype equivalence relation*.

In the model of RAG an affine transformation operates on the domain or space of inputs $\mathbf{x} = (x_1, \dots, x_n)$ to produce the output $\mathbf{y} = \mathbf{x}\mathbf{A} \oplus \mathbf{c}$, which might be used as an input in a function g . Its output $g(\mathbf{y})$ together with the function variables x_1, \dots, x_n are linearly combined by a range transformation which defines the image $f(\mathbf{x})$ as follows:

$$(1) \quad f(\mathbf{x}) = g(\mathbf{y}) \oplus a_1 x_1 \oplus \dots \oplus a_n x_n \oplus d = g(\mathbf{x}\mathbf{A} \oplus \mathbf{c}) \oplus \mathbf{a}^t \mathbf{x} \oplus d$$

where d and a_i for $i = 1, \dots, n$ are constants from Z_k .

Such a transformation belongs to RAG if \mathbf{A} is a non-singular matrix. The name RAG was given to this group by R. Lechner in 1963 (see [8]) and it was studied by Ninomiya (see [12]) who gave the name "prototype equivalence" to the relation it induces on the function space P_k^n .

We want to extract basic facts about some of the subgroups of RAG which are "neighbourhoods" or "relatives" of our transformation groups - IM_k^n , SB_k^n and SP_k^n .

First, we consider a group which is called CA_k^n (complement arguments) and each transformation $\mathbf{j} \in CA_k^n$ is determined by an n -tuple from Z_k^n , i.e. $CA_k^n = \{(j_1, \dots, j_n) \in Z_k^n\}$. Intuitively, CA_k^n will complement some of the variables of a function. If $\mathbf{j} = (j_1, \dots, j_n)$ is in CA_k^n , define $\mathbf{j}(x_1, \dots, x_n) = (x_1 \oplus j_1, \dots, x_n \oplus j_n)$. The group operation is sum mod k and written \oplus . For example if $n = k = 3$ and $\mathbf{j} = (2, 1, 0)$ then $\mathbf{j}(x_1, x_2, x_3) = (x_1 \oplus 2, x_2 \oplus 1, x_3)$ and \mathbf{j} induces a permutation on $Z_3^3 = \{0, 1, 2\}^3$. Then the following sequence of images: $\mathbf{j} : 000 \rightarrow 210 \rightarrow 120 \rightarrow 000$ determines the cycle $(0, 21, 15)$ and if we agree to regard each triple from Z_3^3 as a ternary number, then the permutation induced by \mathbf{j} can be written in cyclic notation as $(0, 21, 15)(1, 22, 16)(2, 23, 17)(3, 24, 9)(4, 25, 10)(5, 26, 11)(6, 18, 12)(7, 19, 13)(8, 20, 14)$. In [6] M. Harrison showed that the boolean functions of two variables are grouped into seven classes under the group CA_2^2 .

Another classification occurs when permuting arguments. If $\pi \in S_n$ then π acts on variables by: $\pi(x_1, \dots, x_n) = (x_{\pi(1)}, \dots, x_{\pi(n)})$. Each permutation induces a map on the domain Z_k^n . For instance the permutation $\pi = (1, 2)$ induces a permutation on $\{0, 1, 2\}^3$ when considering the algebra P_3^3 . Then we have $\pi : 010 \rightarrow 100 \rightarrow 010$ and in cyclic notation it can be written as

$$(3, 9)(4, 10)(5, 11)(6, 18)(7, 19)(8, 20)(15, 21)(16, 22)(17, 23).$$

S_k^n denotes the transformation group induced by permuting of variables. It is clear that S_k^n is isomorphic to S_n .

If we allow both complementations and permutations of the variables, then a transformation group, called G_k^n , is induced. The group action on variables is

TABLE 2. Classes in P_2^2 under RAG .

$[0, 1, x_1, x_2, x_1^0, x_2^0, x_1 \oplus x_2, x_1 \oplus x_2^0]$
$[x_1x_2, x_1x_2^0, x_1^0x_2, x_1^0x_2^0, x_1 \oplus x_1x_2, x_2^0 \oplus x_1x_2, x_1^0 \oplus x_1x_2, x_1^0 \oplus x_1x_2^0]$

TABLE 3. Subgroups of RAG

Subgroup	Equivalence relations	Determination
RAG	Prototype equivalence	A -non-singular
GE_k^n	genus	A = P , a = 0
CF_k^n	complement function	A = I , a = 0 , c = 0
A_k^n	affine transformation	a = 0 , $d = 0$
G_k^n	permute & complement variables (symmetry types)	A = P , a = 0 , $d = 0$
LF_k^n	add linear function	A = I , c = 0 , $d = 0$
CA_k^n	complement arguments	A = I , a = 0 , $d = 0$
LG_k^n	linear transformation	c = 0 , a = 0 , $d = 0$
S_k^n	permute variables	A = P , c = 0 , a = 0 , $d = 0$

represented by $((j_1, \dots, j_n), \pi)(x_1, \dots, x_n) = (x_{\pi(1)} \oplus j_1, \dots, x_{\pi(n)} \oplus j_n)$ where $j_m \in Z_k$ for $1 \leq m \leq n$ and $\pi \in S_n$. The group G_2^n is especially important in switching theory and other areas of discrete mathematics, since it is the symmetry group of the n -cube. The classification of the boolean functions under G_2^2 into six classes is shown in [6].

Let us allow a function to be equivalent to its complements as well as using equivalence under G_k^n . Then the transformation group which is induced by this equivalence relation is called the *genera* of G_k^n and it is denoted by GE_k^n . Thus the equivalence relation \simeq_{gen} which induces genera of G_k^n is defined as follows $f \simeq_{gen} g \iff f \simeq_{G_k^n} g$ or $f = g \oplus j$ for some $j \in Z_k$. Then there exist only four equivalence classes in P_2^2 , induced by GE_2^2 . These classes are the same as the classes induced by the group IM_2^2 in the algebra P_2^2 (see [6] and Table 1, given above).

Next important classification is generated by equivalence relations which allow adding linear or affine functions of variables. In order to preserve the group property we shall consider invertible linear transformations and assume that k is a prime number such that LG_k^n the general linear group on an n -dimensional vector space is over the field Z_k . The transformation groups LG_2^n and A_2^n of linear and affine transformations in the algebra of boolean functions are included in the lattice of the subgroups of RAG . We extend this view to the functions from P_k^n . The algebra of boolean functions in the simplest case of two variables is classified in eight classes under LG_2^2 and in five classes under A_2^2 . Table 2 presents both equivalence classes of boolean functions from P_2^2 under the transformation group RAG .

The subgroups of RAG defined above are determined by equivalence relations as it is shown in Table 3, where **P** denotes a permutation matrix, **I** is the identity matrix, **b** and **c** are vectors from Z_k^n and $d \in Z_k$.

It is naturally to ask which subgroups of RAG are subgroups of the groups IM_k^n or SB_k^n . The answer of this question is our next goal.

Example 4.1. Let $f = x_1x_2^0x_3 \oplus x_1^0$ and $g = x_1x_2^0x_3 \oplus x_1x_2$ be two boolean functions. Then

$$\text{sub}_1(f) = \text{sub}_1(g) = 3, \text{sub}_2(f) = \text{sub}(g) = 3 \quad \text{and} \quad \text{sub}_3(f) = \text{sub}_3(g) = 1.$$

Hence $f \simeq_{\text{sub}} g$. In a similar way, it can be shown that $f \simeq_{\text{imp}} g$. The details are left to the reader.

On the other side, one can prove that there is no transformation $\varphi \in \text{RAG}$ such that $\varphi(x_1^0) = x_1x_2$ (see Table 2) and hence there is no affine transformation $\varphi \in \text{RAG}$ for which $g = \varphi(f)$.

Consequently, each group among IM_k^n , SB_k^n and SP_k^n can not be a subgroup of RAG .

Table 3 allows us to establish the following fact.

Fact 4.1. If f and g satisfy (1) with $\mathbf{A} \notin \{\mathbf{0}, \mathbf{P}, \mathbf{I}\}$ or $\mathbf{a} \neq \mathbf{0}$ then $f \not\simeq_{\text{imp}} g$, $f \not\simeq_{\text{sub}} g$ and $f \not\simeq_{\text{sep}} g$.

Proposition 4.2.

- (i) $\text{LG}_k^n \not\leq \text{SP}_k^n$; (ii) $\text{LF}_k^n \not\leq \text{SP}_k^n$;
- (iii) $\text{IM}_k^n \not\leq \text{RAG}$; (iv) $\text{SB}_k^n \not\leq \text{RAG}$.

Proof. Immediate from Fact 4.1 and Example 4.1. □

Let $\sigma : Z_k \rightarrow Z_k$ be a mapping and $\psi_\sigma : P_k^n \rightarrow P_k^n$ be a transformation of P_k^n determined by σ as follows $\psi_\sigma(f)(\mathbf{a}) = \sigma(f(\mathbf{a}))$ for all $\mathbf{a} = (a_1, \dots, a_n) \in Z_k^n$.

Theorem 4.2. $\psi_\sigma \in \text{IM}_k^n$ and $\psi_\sigma \in \text{SB}_k^n$ if and only if σ is a permutation of Z_k , $k > 2$.

Proof. " \Leftarrow " Let $\sigma \in S_{Z_k}$ be a permutation of Z_k and let f be an arbitrary function with $\text{ess}(f) = n \geq 0$. We shall proceed by induction on n , the number of essential variables in f .

If $n = 0$ then clearly $\psi_\sigma(f)$ is a constant and hence $f \simeq_{\text{imp}} \psi_\sigma(f)$ and $f \simeq_{\text{sub}} \psi_\sigma(f)$.

Assume that if $n < p$ then $f \simeq_{\text{imp}} \psi_\sigma(f)$ and $f \simeq_{\text{sub}} \psi_\sigma(f)$ for some natural number $p, p > 0$. Hence $f(x_i = j) \simeq_{\text{imp}} \psi_\sigma(f(x_i = j))$ and $\text{sub}_m(f(x_i = j)) = \text{sub}_m(\psi_\sigma(f(x_i = j)))$ for all $i \in \{1, \dots, n\}$, $m \in \{1, \dots, n-1\}$ and $j \in Z_k$.

Let $n = p$. Let $x_i \in \{x_1, \dots, x_n\} = \text{Ess}(f)$ and $j \in Z_k$, and let us set $g = f(x_i = j)$. Then $\psi_\sigma(g) = \psi_\sigma(f(x_i = j))$ and $\text{ess}(g) = n - 1 < p$. Hence our inductive assumption implies $g \simeq_{\text{imp}} \psi_\sigma(g)$ and $g \simeq_{\text{sub}} \psi_\sigma(g)$. Consequently, we have

$$f(x_i = j) \simeq_{\text{imp}} \psi_\sigma(f(x_i = j)) \quad \text{and} \quad \text{sub}_m(f(x_i = j)) = \text{sub}_m(\psi_\sigma(f(x_i = j)))$$

for all $x_i \in \{x_1, \dots, x_n\}$ and $j \in Z_k$, which shows that $f \simeq_{\text{imp}} \psi_\sigma(f)$ and $f \simeq_{\text{sub}} \psi_\sigma(f)$.

" \Rightarrow " Let us assume that σ is not a permutation of Z_k . Hence there exist two constants a_1 and a_2 from Z_k such that $a_1 \neq a_2$ and $\sigma(a_1) = \sigma(a_2)$. Let us fix the vector $\mathbf{b} = (b_1, \dots, b_n) \in Z_k^n$. Then we define the following function from P_k^n :

$$f(x_1, \dots, x_n) = \begin{cases} a_1 & \text{if } x_i = b_i \text{ for } i = 1, \dots, n \\ a_2 & \text{otherwise.} \end{cases}$$

Clearly, $\text{Ess}(f) = X_n$. On the other hand the range of f is $\text{range}(f) = \{a_1, a_2\}$ and $\sigma(\text{range}(f)) = \{\sigma(a_1)\}$, which implies that $\psi_\sigma(f)(c_1, \dots, c_n) = \sigma(a_1)$ for all

$(c_1, \dots, c_n) \in Z_k^n$. Hence $\psi_\sigma(f)$ is the constant $\sigma(a_1) \in Z_k$ and $Ess(\psi_\sigma(f)) = \emptyset$. Thus we have $f \not\simeq_{imp} \psi_\sigma(f)$ and $f \not\simeq_{sub} \psi_\sigma(f)$. \square

Theorem 4.3. *Let $\pi \in S_n$ and $\sigma_i \in S_{Z_k}$ for $i = 1, \dots, n$. Then $f(x_1, \dots, x_n) \simeq_{imp} f(\sigma_1(x_{\pi(1)}), \dots, \sigma_n(x_{\pi(n)}))$ and $f(x_1, \dots, x_n) \simeq_{sub} f(\sigma_1(x_{\pi(1)}), \dots, \sigma_n(x_{\pi(n)}))$.*

Proof. Let $f \in P_k^n$ be an arbitrary function and assume $Ess(f) = X_n$.

First, we shall prove that

$$f(x_1, \dots, x_n) \simeq_{imp} f(x_{\pi(1)}, \dots, x_{\pi(n)})$$

and

$$f(x_1, \dots, x_n) \simeq_{sub} f(x_{\pi(1)}, \dots, x_{\pi(n)}).$$

Let $g = f(x_{\pi(1)}, \dots, x_{\pi(n)})$. Clearly, if $n \leq 1$ then $f \simeq_{imp} g$ and $f \simeq_{sub} g$. Assume that if $n < p$ then $f \simeq_{imp} g$ and $f \simeq_{sub} g$ for some natural number $p, p \geq 1$.

Let us suppose $n = p$. Let $x_i \in Ess(f)$ be an arbitrary essential variable in f and let $c \in Z_k$ be an arbitrary constant from Z_k . Then we have

$$\begin{aligned} f(x_i = c)(x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_p) &= \\ &= g(x_{\pi^{-1}(i)} = c)(x_{\pi^{-1}(1)}, \dots, x_{\pi^{-1}(i-1)}, x_{\pi^{-1}(i+1)}, \dots, x_{\pi^{-1}(p)}). \end{aligned}$$

Our inductive assumption implies $f(x_i = c) \simeq_{imp} g(x_{\pi(i)} = c)$ and $sub_m(f(x_i = c)) = sub_m(g(x_{\pi(i)} = c))$ for all $x_i \in X_n, m \in \{1, \dots, p-1\}$ and $c \in Z_k$. Hence $f \simeq_{imp} g$ and $f \simeq_{sub} g$.

Second, let us prove that

$$f(x_1, \dots, x_n) \simeq_{imp} f(\sigma_1(x_1), \dots, \sigma_n(x_n))$$

and

$$f(x_1, \dots, x_n) \simeq_{sub} f(\sigma_1(x_1), \dots, \sigma_n(x_n)).$$

Let $h = f(\sigma_1(x_1), \dots, \sigma_n(x_n))$. Then we have

$$f(a_1, \dots, a_n) = h(\sigma_1^{-1}(a_1), \dots, \sigma_n^{-1}(a_n)).$$

Hence, if $(i_1 \dots i_r, a_{i_1} \dots a_{i_r}, c) \in Imp(f)$ then $(i_1 \dots i_r, \sigma_{i_1}^{-1}(a_{i_1}) \dots \sigma_{i_r}^{-1}(a_{i_r}), c) \in Imp(h)$ for some $r, 1 \leq r \leq n$. Since σ_i is a permutation of Z_k for $i = 1, \dots, n$ it follows that $f \simeq_{imp} h$. By similar arguments it follows that $f \simeq_{sub} h$. \square

Corollary 4.1. (i) $GE_k^n \leq IM_k^n$; (ii) $GE_k^n \leq SB_k^n$; (iii) $GE_k^n \leq SP_k^n$.

5. CLASSIFICATION OF BOOLEAN FUNCTIONS

In this section we compare a collection of subgroups of RAG with the groups of transformations preserving the relations \simeq_{imp} , \simeq_{sub} and \simeq_{sep} and to obtain estimations for the number of equivalence classes, and for the cardinalities of these classes in the algebra of Boolean functions. Our results are based on Proposition 4.2, Theorem 4.2 and Theorem 4.3. Thus we have

$$(2) \quad GE_2^n \leq IM_2^n, \quad GE_2^n \leq SB_2^n, \quad LG_2^n \not\leq SP_2^n \quad \text{and} \quad LF_2^n \not\leq SP_2^n.$$

These relationships determine the places of the groups IM_2^n , SB_2^n and SP_2^n with respect to the subgroups of RAG. Figure 4 shows the location of these groups together with the subgroups of RAG.

M. Harrison [6] and R. Lechner [7] counted the number of equivalence classes and the cardinalities of the classes under some transformation subgroups of RAG for Boolean functions of 3 and 4 variables.

The relations (2) show that if we have the values of $t(GE_2^n)$ then we can count the numbers $t(IM_2^n)$, $t(SB_2^n)$ and $t(SP_2^n)$ because the equivalence classes under these transformation groups are union of equivalence classes under GE_2^n and hence we have $t(IM_2^n) \leq t(GE_2^n)$ and $t(SB_2^n) \leq t(GE_2^n)$. Moreover, if we know the factor-set P_2^n / \simeq_{gen} of representative functions under \simeq_{gen} then we can effectively calculate the sets P_2^n / \simeq_{imp} , P_2^n / \simeq_{sub} and P_2^n / \simeq_{sep} because of $P_2^n / \simeq_{imp} \subseteq P_2^n / \simeq_{gen}$ and $P_2^n / \simeq_{sub} \subseteq P_2^n / \simeq_{gen}$.

The next theorem allows us to count the number $imp(f)$ of the implementations of any function f by a recursive procedure. Such a procedure is realized and its execution is used when calculating the number of the implementations and classifying the functions under the equivalence \simeq_{imp} .

Theorem 5.1. *Let $f \in P_2^n$ be a boolean function. The number of all implementations in f is determined as follows:*

$$imp(f) = \begin{cases} 1 & \text{if } ess(f) = 0 \\ 2 & \text{if } ess(f) = 1 \\ \sum_{x \in Ess(f)} [imp(f(x=0)) + imp(f(x=1))] & \text{if } ess(f) \geq 2. \end{cases}$$

Proof. We shall proceed by induction on $n = ess(f)$ - the number of essential variables in f . The lemma is clear if $ess(f) = 0$. If f depends essentially on one variable x_1 , then there is a unique BDD of f with one non-terminal node which has two outgoing edges. These edges together with the labels of the corresponding terminal nodes form the set $Imp(f)$ of all implementations of f , i.e. $imp(f) = 2$.

Let us assume that

$$imp(f) = \sum_{i=1}^n [imp(f(x_i=0)) + imp(f(x_i=1))]$$

if $n < s$ for some natural number s , $1 \leq s$.

Next, let us consider a function f with $ess(f) = s$. Without loss of generality, assume that $Ess(f) = \{x_1, \dots, x_n\}$ with $n = s$. Since $x_i \in Ess(f)$ for $i = 1, \dots, n$ it follows that $f(x_i=0) \neq f(x_i=1)$ and there exist BDDs of f whose label of the first non-terminal node is x_i . Let D_f be a such BDD of f and let $(ij_2 \dots j_m, c_1 c_2 \dots c_m c) \in Imp(f)$ with $m \leq n$. Hence

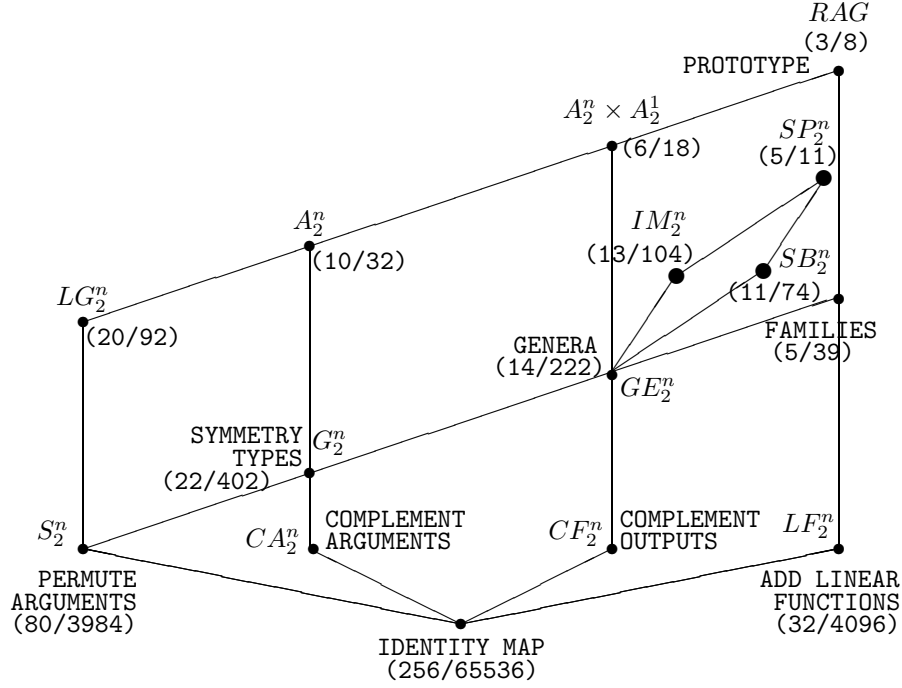
$$(j_2 \dots j_m, c_2 \dots c_m c) \in Imp(g)$$

where $g = f(x_i = c_1)$. On the other side it is clear that if $(j_2 \dots j_m, d_2 \dots d_m d) \in Imp(g)$ then $(ij_2 \dots j_m, c_1 d_2 \dots d_m d) \in Imp(f)$. Consequently, there is an one-to-one mapping between the set of implementations of f with first variable x_i and first edge labelled by c_1 , and $Imp(g)$, which completes the proof. \square

We also develop recursive algorithms to count $sub_m(f)$ and $sep_m(f)$ for $f \in P_2^n$, presented below.

Table 4 shows the number of equivalence classes under the equivalence relations induced by the transformation groups G_2^n , IM_2^n , SB_2^n and SP_2^n for $n = 1, 2, 3, 4$. M. Harrison found from applying Polya's counting theorem (see [6]) the numbers $t(G_2^5)$ and $t(G_2^6)$, which are upper bounds of $t(IM_2^n)$, $t(SB_2^n)$ and $t(SP_2^n)$ for $n = 5, 6$.

Figure 4 and Table 5 show that for the algebra P_2^3 there are only 14 different generic equivalent classes, 13 imp-classes, 11 sub-classes and 5 sep-classes. Hence

FIGURE 4. Transformation groups in P_2^n ($n = 3/n = 4$)TABLE 4. Number of classes under *symmetry type*, \simeq_{imp} , \simeq_{sub} and \simeq_{sep}

n	$t(G_2^n)$	$t(IM_2^n)$	$t(SB_2^n)$	$t(SP_2^n)$
1	3	2	2	2
2	6	4	4	3
3	22	13	11	5
4	402	104	74	11
5	1 228 158	1606	< 1228158	38
6	400 507 806 843 728	< 400 507 806 843 728		

three mappings that converts each generic class into an imp-class, into a sub-class and into a sep-class are required. Each generic class is a different row of Table 5. For example, the generic class №12 (as it is numbered in Table VIII, [7]) is presented by 10-th row of Table 5. It consists of 8 functions obtained by complementing function f and/or permuting and/or complementing input variables in all possible ways, where $f = x_1x_2^0x_3 \oplus x_1x_2x_3^0 \oplus x_2x_3$. This generic class №12 is included in imp-class №9, sub-class №8 and sep-class №5 which shows that $imp(f) = 36$, $sub(f) = 12$ and $sep(f) = 7$. The average cardinalities of equivalence classes and complexities of functions are also shown in the last row of Table 5.

Table 6 shows the *sep*-classes of boolean functions depending on at most five variables. Note that there are $2^{32} = 4294967296$ functions in P_2^5 . All calculations were performed on a computer with two Intel Xeon E5/2.3 GHz CPUs. The execution with total exhaustion took 244 hours.

TABLE 5. Classification of P_2^3 under \simeq_{sep} , \simeq_{sub} , \simeq_{imp} and genus.

sep-class №	$sep(f)$	func. per class	sub-class №	$sub(f)$	func. per class	imp-class №	$imp(f)$	func. per class	Generic class [7] №	func. per class	representative function f
1	0	2	1	1	2	1	1	2	1	2	0
2	1	6	2	3	6	2	2	6	9	6	x_1
3	3	30	3	5	24	3	6	24	3	24	x_1x_2
			4	7	6	4	8	6	10	6	$x_1 \oplus x_2$
4	6	24	5	11	24	5	28	24	13	24	$x_1 \oplus x_1x_3 \oplus x_2x_3$
5	7	194	6	9	64	6	21	16	2	16	$x_1x_2x_3$
						7	23	48	6	48	$x_1x_2x_3^0 \oplus x_1$
			7	12	48	8	30	48	7	48	$x_1x_2x_3^0 \oplus x_2x_3$
											$x_1x_2x_3^0 \oplus x_1x_2x_3^0 \oplus x_2x_3$
			8	12	8	9	36	16	12	8	$x_1x_2x_3^0 \oplus x_1x_2x_3^0 \oplus x_2x_3$
											$x_1^0x_2x_3 \oplus x_1x_2^0x_3^0$
			9	15	26	10	42	16	8	16	$x_1x_2x_3^0 \oplus x_1^0x_2x_3$
											$x_1 \oplus x_2 \oplus x_3$
			10	13	24	11	48	2	11	2	$x_1 \oplus x_2x_3$
											$x_1x_2^0x_3 \oplus x_1x_2x_3^0$
aver.	6.2	51.2		10.6	23.3		26.0	19.7		18.3	

TABLE 6. Classes in P_2^5 under \simeq_{sep}

sep- class №	$sep_5(f)$	$sep_4(f)$	$sep_3(f)$	$sep_2(f)$	$sep_1(f)$	$sep(f)$	functions per class
1	0	0	0	0	0	0	2
2	0	0	0	0	1	1	10
3	0	0	0	1	2	3	100
4	0	0	1	2	3	6	240
5	0	0	1	3	3	7	1940
6	0	1	2	5	4	12	1920
7	0	1	3	4	4	12	2400
8	0	1	3	5	4	13	8160
9	0	1	4	4	4	13	120
10	0	1	4	5	4	14	8400
11	0	1	4	6	4	15	301970
12	1	2	7	9	5	24	20480
13	1	3	5	7	5	21	3840
14	1	3	5	8	5	22	9600
15	1	3	6	6	5	21	1920
16	1	3	6	7	5	22	1920
17	1	3	6	8	5	23	38400
18	1	3	7	7	5	23	1920
19	1	3	7	8	5	24	38400
20	1	3	7	9	5	25	130560
21	1	4	6	6	5	22	3000
22	1	4	7	7	5	24	34720
23	1	4	7	8	5	25	177120
24	1	4	7	9	5	26	274560
25	1	4	8	7	5	25	7680
26	1	4	8	8	5	26	274560
27	1	4	8	9	5	27	1847280
28	1	5	7	9	5	27	81920
29	1	5	8	8	5	27	600
30	1	5	8	9	5	28	1013760
31	1	5	8	10	5	29	38400
32	1	5	9	7	5	27	1200
33	1	5	9	8	5	28	449040
34	1	5	9	9	5	29	4093200
35	1	5	9	10	5	30	5443200
36	1	5	10	8	5	29	13680
37	1	5	10	9	5	30	5826160
38	1	5	10	10	5	31	4274814914

REFERENCES

- [1] R. E. Bryant, Graph-based algorithms for Boolean function manipulation. *IEEE Transactions on Computers*, **C-35(8)**, (1986), pp. 677-691.
- [2] Y. Breitbart, Essential variables of Boolean Function, (Russian), *Dokl. Akad.Nauk SSSR*, **172**, 1, (1967), pp. 9-10.
- [3] K. Chimev, Separable sets of arguments of functions, *MTA SzTAKI Tanulmányok, Budapest*, **(80)**, (1986), 173 p.
- [4] Complexity of Boolean functions, *Seminar 06111*, (2006), <http://drops.dagstuhl.de/opus/volltexte/2006/840/pdf/BoolFunc06ExSum.840.pdf>
- [5] I. Damyanov, On some properties of Boolean functions and their binary decision diagrams, *Mathematics and Education in Mathematics, Proc. of the 40th Spring Conference of the UBM, Borovets*, (2011), pp. 61-71.
- [6] M.Harrison, Counting theorems and their applications to classification of switching functions, *Recent Developments in Switching Theory*, (ed. A. Mikhopadhyay), NY, Academic Press, (1971), pp. 85-120.
- [7] R. J. Lechner, Harmonic analysis of switching functions, *Recent Developments in Switching Theory*, (ed. A. Mikhopadhyay), NY, Academic Press, (1971), pp. 121-228.
- [8] R. J. Lechner, Affine equivalence of switching functions, *Ph.D. Thesis, Harvard Univ., Cambridge, Massachusetts*, (1963).
- [9] O. B. Lupanov, On a class of schema of functional elements.(Russian) *Problemy Kibernet.* **7**, (1962), pp. 61-114.
- [10] D. M. Miller and R. Drechsler, On the construction of multiple-valued decision diagrams, *Proc. 32nd Int. Symp. on Multiple-Valued Logic* (2002), pp. 245-253.
- [11] D. M. Miller, Multiple-valued logic design tools, *Proc. 23rd Int. Symp. on Multiple-Valued Logic* (1993), pp. 2-11.
- [12] I. Ninomiya, A theory of the coordinate representation of switching functions, *Met. Fac. Eng., Nagoya University*, **10(2)**, (1958), pp. 175-190.
- [13] A. Salomaa, On Essential variables of functions, especially in the algebra of logic, *Annales Academia Scientiarum Fennicae*, Ser. A, **333**, (1963), pp. 1-11.
- [14] Sl. Shtrakov, On the separable and annulling sets of variables for the functions, *MTA SzTAKI Kozlmenyek, Budapest*, **35**, (1986), pp. 147-168.
- [15] Sl. Shtrakov, Extremal subsets and coverings of the sets of variables for the functions, *MTA SzTAKI Kozlmenyek, Budapest*, **38**, (1988), pp. 27-35.
- [16] I. Strazdins, On fundamental transformation groups in the algebra of logic, *Colloq. Math. Soc. J. Bolyai*, **28**, Szeged, (1979), pp. 669-691.

DEPARTMENT OF COMPUTER SCIENCE,, SOUTH-WEST UNIVERSITY, BLAGOEVGRAD, BULGARIA,
 DEPARTMENT OF COMPUTER SCIENCE,, SOUTH-WEST UNIVERSITY, BLAGOEVGRAD, BULGARIA,